International Journal of Industrial Engineering & Technology (IJIET)
ISSN(P): 2277-4769; ISSN(E): 2278-9456
Vol. 3, Issue 4, Dec 2013, 5-12

SECURE VHF/UHF COMMUNICATION USING CHAOS SIGNAL GENERATOR

K. AANANDHA SARAVANAN, M. NITHYAVELAM, T. SHANKAR RAJ & C. MALATHI

Department of Electronics and Communication Engineering, Veltech Dr. RR & Dr. SR Technical University, Chennai, India

ABSTRACT

The nonlinear phenomenon is the complex, random-like behaviour, which is being addressed in various fields of research in communication. In this paper we use to prove the harness effects of chaotic signals in Aerospace Communication and apply them to ground to air Communication in VHF/UHF band. Some of the most promising issues involve privacy and security for processing communication signals. There are also potential applications involving military, radar and sonar with important implications for addressing such challenges as urban warfare and the remote detection of improvised explosive devices and suicide bombers. This practice is evolving on many fronts and levels, reaching a state of maturity where it can be applied to real-world problems.

KEYWORDS: Chaos, Nonlinear, Synchronization

INTRODUCTION

Chaos is a branch of the interesting nonlinear systems, exhibits an interesting nonlinear phenomenon and has been intensively studied in the past four decades. Initially, it was studied by researchers with strong mathematical background rather than circuit-designers or electronic engineers/scientists. This is mainly due to the fact that circuit design and implementation cannot match up with the mathematical equations needed due to technical and practical problems. With the advance in circuit technology and digital signal processing in the past few decades, the use of chaos phenomena in daily real-life engineering products become possible. Various applications and products were reported, including but not limited to the following; utilizing the advantage of chaotic dynamic behavior in washing machine technologies, reaction rate control in chemical technologies, treating cardiac arrhythmia and providing a secure communication channel by using a chaotic carrier. Therefore, more and more applications have utilized chaos theory. We are particularly interested in the area of secure communications. Chaotic signals in the time domain are neither periodic nor quasi-periodic and are unpredictable on the long term.

Chaos is a phenomenon that occurs widely in dynamical systems. From educational point of view this phenomenon was considered to be complex and was never given importance cause there was no simple analysis available, which could help students to delve into this interesting phenomenon and get some hands on experience. In the current scenario, since the presence of chaos is being realized in many fields, it is good to have some insight into this phenomenon right from. In this paper we develop this phenomenon using a circuit called Chua circuit. The criterion for choosing Chua's circuit is its simplicity, though simple, it exhibits a variety of chaotic phenomena exhibited by other complex circuits, which makes it a popular circuit. There are two types of chaotic systems, autonomous and non autonomous. Chua's circuit is an autonomous system because there is no external signal injected into the system. In this work, we show how to build Chua's circuit using off-shelf components, describe the design methodology for constructing the nonlinear resistor and present the experimental and simulation results of the Chua's circuit. Chaotic phenomenon can be used in real world

applications like secure communication, medical field, fractal theory and many more. This paper discusses in brief the application of chaos in secure communication

BACKGROUND

There is no precise definition of chaos except that chaos is a form of controlled oscillations, often appearing to be time shifted resonances. Chaos has the form of random oscillations in time with non uniformity in amplitude but essentially stable frequency characteristics. Study of chaos in the modern era dates back to late 1950s when experiments were conducted to study chaotic behavior using circuits, forced vibrations of shallow water waves in a finite container, hydro dynamical instabilities, chemical turbulence, and acousto-optic (A-O) turbulence. Early experiments on chaos were conducted by Faraday using forced vibrations of shallow water waves in a finite container, the vibrations were driven into chaos when a component at a frequency f0/2 in shallow water was observed when the medium was excited with a frequency of f0. This was the likely demonstration of the first existence of chaos. Conducting experiments using shallow water waves was expensive, used a lot of equipment and was difficult to analyze. The next set of experiments included the use of nonlinear circuits.

PROBLEM STATEMENT

In Modern day communication techniques are often prone to hacking and disturbances in the communication system while in transit from one place to another. Signal encryption using chaotic waves may be a good solution to this problem. A modulation scheme uses a carrier frequency to be modulated by the signal waveform, and generally the message can be readily decoded. A chaotic signal is a non-deterministic signal and not a well defined sinusoid. Hence, a modulated chaos wave is secure and cannot be decoded without knowledge of the chaos parameters.

A chaotic signal is generated by carefully choosing the right set of parameters such as feedback gain, bias input and time delay. Encrypting a wave using a chaotic wave as a carrier also depends critically on these parameters. A signal used to encrypt a chaotic carrier can only be recovered or decoded by knowing exactly three parameter set, viz., the bias input 0, feedback gain and time delay Td. Thus, the transmitter parameters serve as a decoding key, and hence signal encryption using a chaotic carrier provides data-security and reliability.

In this research, we examine signal encryption signal. For this, we generate a chaos signal with average frequency as high as 10MHz that is suitable for practical communication applications. We then examine encryption for different signals using the chaos wave with a set of fixed parameters. Finally, we recover the original signal using the same parameter set at the receiver and check for its robustness for cases where the receiver keys are mismatched or detuned. We also perform a encryption using a 10 MHz chaos as carrier and successfully decrypt at the receiver using low pass filter.

SECURE CHAOCTIC COMMUNICATION

The block diagram of the secure chaotic Communication system is shown in Figure. One of the main problems faced while in the implementation of the communication system was that of synchronization. Efforts should be taken to perfectly match the chaotic systems at the transmitter and the receiver ends.

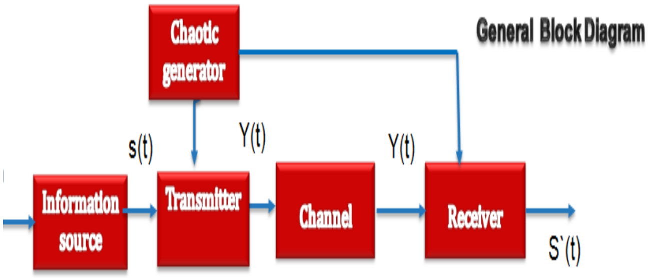

Figure 1

Transmitter Section

The internal block diagram of the transmitter is shown in Figure. The transmitter uses a summer to mask the information signal s(t) with the chaotic signal Vc1(t) generated by the chua's circuit to produce the resultant signal r(t). The buffer is used to get signal without attenuation and the inverter is used transmit the resultant signal without any phase shift

Receiver

The internal block diagram of the receiver is shown in Figure. The receiver consists of a chua's circuit similar to the one at the transmitter to generate a chaotic signal Vc1(t) that is perfectly matched with the chaotic signal generated at the transmitter. The signal r(t) from the transmitter and the chaotic signal Vc1(t) generated from the receiver chaotic system (chua's circuit) are passed through a subtractor, the output of which is s'(t) = r(t) - Vc1(t), which is the same as the message signal. The buffer is used for coupling to make sure that the signal is not attenuated.

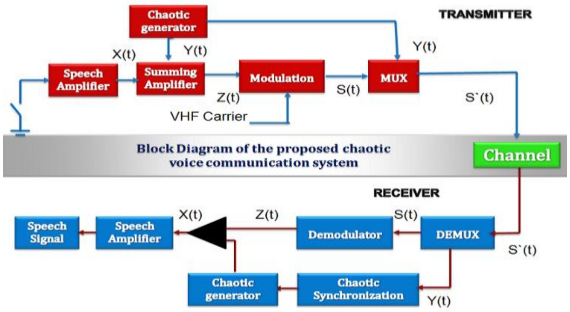

Figure 2

CHAOTIC SIGNAL MASKING

In its simplest form a chaotic masking circuit needs an input signal, a master chaos generator, some sort of summing amplifier, a slave chaos generator, and a difference amplifier

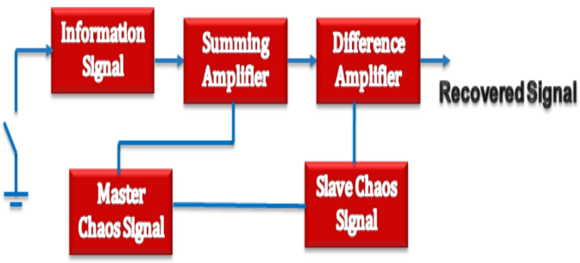

Figure 3

The master chaos generator produces a voltage that when viewed as a 1-D trace on an oscilloscope looks like noise. When added to the original message signal the output should make the message unrecognizable. To recover the signal, an *exact* copy of the master chaos signal needs to be available or the original signal will look noisy. Synchronization of the master generator with a slave ideally made of matched components causes their voltage dynamics to become identical which makes it possible to replicate the unique chaotic masking waveform in real time that would otherwise be impossible to achieve. By subtracting the slave signal with the master and the original, theoretically an exact copy of the original will be recovered. The ability for chaotic circuits to synchronize is why they're of interest to those working in encryption and other types of secured communication.

CHAOTIC SYNCHRONIZATION

The classical synchronization or entrainment of periodic oscillators has been known since at least the seventeenth century, when Christian Huygens observed the coupled form of this phenomenon in adjacent clocks on a wall. The driven or injection form of synchronization was discovered later with the observation that a small periodic forcing signal could cause the large natural resonance of a system to lock to it. What was unexpected was that a similar phenomenon could be had with chaotic signals, especially given their distinctive bounded instability character. The discovery of the driven form of chaotic synchronization was announced in 1990, marking a turning point in the investigation of chaos for communication systems, for it allowed chaos to be modulated and demodulated like a generalized carrier.

There are five basic chaotic synchronization techniques, all of which relate to communication applications that are generic across national security space programs:

- **Master-Slave Synchronization.** This was the earliest discovered version of chaotic synchronization. It occurs when an autonomous (that is, unforced) system unidirectionally drives a stable subsystem.
- **Nonautonomous Synchronization.** Here, a nonautonomous (that is, forced) system unidirectionally drives a stable identical nonautonomous system. This form is known to be quite robust against link interference.
- **Inverse System Synchronization.** In contrast to nonautonomous synchronization, inverse system synchronization occurs when the receiver is a formal dynamical inverse of the transmitter that will reproduce the latter's forcing function.
- **Adaptive Control Synchronization.** By far the most prolific class of synchronization approaches, this is based on the numerous variants of adaptive control for chaotic systems (also known as "control chaos"). In fact, these techniques have demonstrated some capability (although easily defeated) of extracting information from unknown systems, or even making distinctly different dynamical systems synchronize, thereby possibly weakening the security claims often made for chaos-based communications. These techniques can also make the other forms of chaotic synchronization more suitable for practical implementation—for example, where there are link degradations and parameter mismatches.
- **Coupled Synchronization.** This consists of bidirectionally coupled identical systems and is a simple generalization of the traditional classical form involving sinusoidal oscillators.

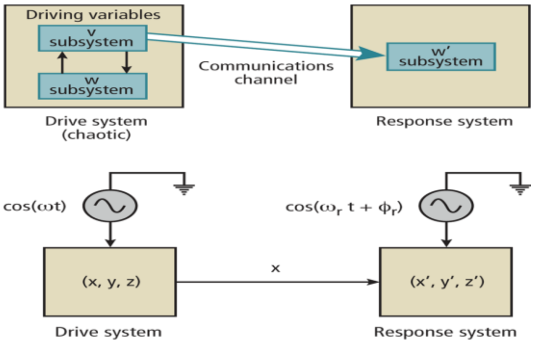

Figure 4: Chaotic Synchronization

The first four forms of chaotic synchronization are suitable for standard communications purposes, while the fifth is suitable for network communications. It is also preferable that the linking signal between the component systems be of the scalar variety. Because of the newness of these discoveries, many studies are still needed to address important engineering and operational issues, and to compare findings with traditional synchronization approaches.

CHAOS CIRCUIT AND SIMULATION

A fully realized circuit can be built from only resistors, capacitors and op-amps. These circuit components can be found lying around in most labs and are readily available off the shelf in any RadioShack .All op-amps used are TL082. Each chip has two op-amps--one on either side. You could also use the TL084, which has 4 op-amps, depending on your specific circuit design. L here represents the inductance value of the gyrator, which we are using in place of an actual inductor. Calculating this value can be done as follows:

L=(R7R9R10C)/R8

This gyrator simulates an ideal inductor, and you will see later how this is useful for measuring the signals produced. For capacitors, I highly recommend you avoid the common, round, ceramic capacitors. They work much better and it will make the output much sharper.Precision resistors are not really worth it unless you want really clear and precise double scrolls. Regular resistors work just fine. But you do want to get nice, easy to adjust potentiometers. You will be spending most of your time turning these little dials trying to get the right patterns to show up, and you will thank yourself for not using the screwdriver-adjustable only pots. Get something with big nobs that are easy to tune and have fine control. These circuits are sensitive and you want to have control over what is going on.There are three signals that you will want to measure on the Chua's circuit: X, Y, and Z. X is the voltage across the capacitor C1, Y is the voltage across the capacitor C2, and Z is the current through the inductor. Since we are using a gyrator to simulate the inductor, all we need to do is measure the voltage at point P [Figure B], since we can determine the state vectors from just that. The acutal current through our simulated inductor can be calculated by:

Z=(VP-Y)/R7

If you did everything right, you should be coming up with some sinusoidal waveforms like inFigure C when you hook up to your oscilloscope. Plot them against eachother to see some interesting patterns evolve as you adjust the two potentiometers.

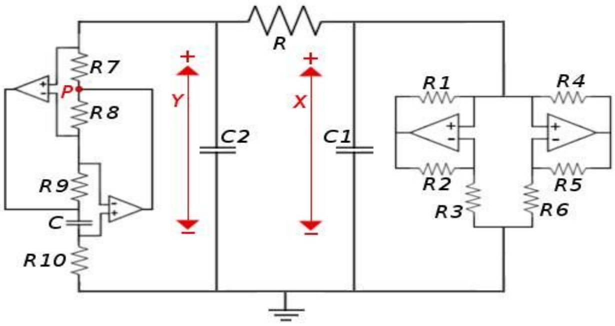

Figure 5

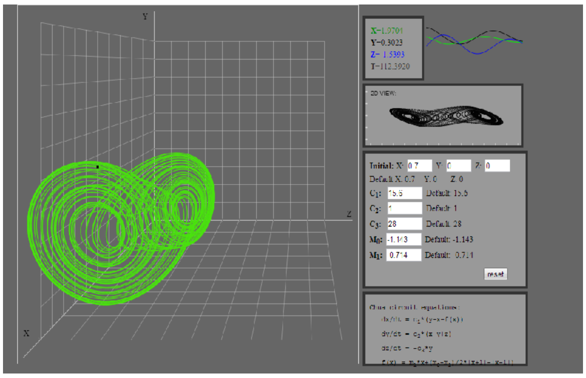

Figure 6: Simulation Result of Chaotic Generator

COUPLING AND SYNSCHRONIZATION

Now we can take synchronization of two or more circuits. By now we know that a chaotic circuit has three states (three signals). One of the beauties of a chaotic circuit is that, if left alone, two circuits will never have the three signals be exactly the same at any point in time (due to the property of 'sensitivity to initial conditions'). In other words, two circuits will never be naturally in sync. But, with a little more circuitry, we can synchronize the two chaotic circuits and the signals will match.Synchronized chaotic circuits are frequently used in real applications. To accomplish basic synchronization of two circuits, we must set up our two circuits with an intermediate coupling circuit as in Figures C and D and realized in Figure B. There are many ways to couple a system for synchronization, the two most popular are bidirectional, and Master/Slave (unidirectional).The Master/Slave approach. In a Master/Slave there is only one Master Chua circuit and the rest are Slaves. The Master Chua is unaffected by the Slave circuits or the coupling and acts autonomously. The Slave Chua circuits use the coupling circuitry to synchronize to the Master's signal. In summary, the Slaves synchronize to the Master Chua, but the Master Chua is unaffected.

CONCLUSIONS

In this paper, an innovative application of chaoctic signal in aerospace communications architecture is shown. This architecture is a design for a nonlinear filter that recovers the information signal injected at the transmitter using parameter modulation. Simulations, we show the effectiveness and general applicability of this design, we demonstrated the practicality of our approach by transmitting and clearly receiving audio signals. These imply that the design is tolerant to system perturbations and typical component mismatch between the transmitter and receiver circuits. This analysis has shown that chaotic masking can be achieved using a very simple circuit design using inexpensive, off the shelf components. These circuits are extremely sensitive and the ultimate goal is to always maintain chaotic dynamics with increasing complexity of the circuit. The system design possesses an interesting attribute that we have not explicitly

illustrated in the simulations. The dynamics of the chaos do not have to be spectrally separated from the information signal for the nonlinear filter to work. Therefore, with the proper choice of the dynamics of the information signal and the chaos can overlap significantly, thereby increasing the security aspects of the communications system.

REFERENCES

1. Hilborn, Robert C. *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*. 2nd ed. Oxford: Oxford University Press, 2000 Print.
2. Berkowitz, Jack, Daniel Klein, and James Wampler. "An Archetypal Chaotic Circuit." 8 Mar. (2012): 1-25. Print.
3. Kennedy, Michael P. "Robust Op Amp Realization of Chua's Circuit." *Frequenz* 46.3-4 Mar. (1992): 66-80. Web. 9 June 2012.
4. *1995 Int. Symp. Circuits Syst. (ISCAS'95),* vols. I–III. Piscataway, NJ:IEEE, Apr. 1995.
5. J. M. Elmirghani, Ed., *SPIE Proc., Chaotic Circuits Commun.,* vol. 2612,Oct. 1995.
6. *1996 Int. Symp. Circuits Syst. (ISCAS'96),* vol. 3. Piscataway, NJ:IEEE, May 1996.
7. H. Dedieu, M. P. Kennedy, and M. Hassler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Circuits Syst. II,* vol. 40, pp. 634–642, Oct. 1993.
8. A.V. Oppenheim, G. W. Wornell, S. H. Isabelle, and K. M. Cuomo,"Signal processing in the context of chaotic signals," in *Proc. IEEEICASSP,* vol. IV, Mar. 1992, pp. 117–120.
9. Lj. Kocarev, K. S. Halle, and K. Eckert, L. O. Chua, and U. Parlitz,"Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurc. Chaos,* vol. 2, no. 3, pp. 709–713, 1992.
10. K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications,"*IEEE Trans. Circuits Syst. II,* vol. 40, pp. 626–633, Oct. 1993.
11. K. M. Short, "Steps for unmasking secure communications," *Int. J.Bifurc. Chaos,* vol. 4, no. 4, pp. 959–977, 1994.
12. U. Parlitz, L. O. Chua, Lj. Kocarev, K. S. Halle, and A. Shang,"Transmission of digital signals by chaotic synchronization," *Int. J.Bifurc. Chaos,* vol. 2, no. 4, pp. 973–977, 1992.
13. P. Celka, "Chaotic synchronization and modulation of nonlinear timedelayed feedback optical systems," *IEEE Trans. Circuits Syst. I,* vol. 42,pp. 455–463, Aug. 1995.
14. T. L. Carroll and L. M. Pecora, "Cascading synchronized chaotic systems," *Phys. D,* vol. 67, pp. 126–140, Aug. 1993.
15. K. S. Halle, C. W. Wu, M. Itoh, and L. O. Chua, "Spread spectrum communication through modulation of chaos," *Int. J. Bifurc. Chaos,* vol.3, no. 2, pp. 469–477, 1993.
16. C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with aplications to secure communications systems," *Int. J.Bifurc. Chaos,* vol. 3, no. 6, pp. 1619–1627, 1993.
17. M. Itoh, H. Murakami, and L. O. Chua, "Communication systems viachaotic modulations," *IEICE Trans. Fundament.,* vol. E77-A, no. 6, pp.1000–1005, June 1994.

18. M. Itoh and H. Murakami, "New communication systems via chaotic synchronizations and modulations," *IEICE Trans. Fundament.*, vol. E78-A, no. 3, pp. 285–290, Mar. 1995.

19. L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems,"*Phys. Rev. Lett.*, vol. 64, pp. 821–824, Feb. 1990.

20. T. L. Carroll and L. M. Pecora, "Synchronizing chaotic circuits," *IEEE Trans. Circuits Syst.*, vol. 38, pp. 453–456, Apr. 1991.

21. M. J. Ogorzalek, "Taming chaos—Part I: Synchronization," *IEEE Trans.Circuits Syst. I*, vol. 40, pp. 693–699, Oct. 1993.

22. M. T. Thompson and H. B. Stewart, *Nonlinear Dynamics and Chaos.*New York: Wiley, 1986.

23. M. Pecora, "Overview of chaos and communications research," *SPIEProc., Chaos Commun.*, vol. 2038, pp. 2–25, July 1993.

24. Ed., *SPIE Proc., Chaos in Commun.*, vol. 2038, July 1993.

25. M. Hasler, "Synchronization principles and applications," in *Circuits and Systems Tutorials*, C. Toumazou, Ed. Piscataway, NJ: IEEE, 1994,pp. 314–327.